Model Checking for Network Security Requirements via a Flexible Modeling Framework

John D. Powell
Jet Propulsion Laboratory, California Institute of Technology
John.Powell@jpl.nasa.gov
David P. Gilliam
Jet Propulsion Laboratory, California Institute of Technology
David.P.Gilliam@jpl.nasa.gov

Abstract

Network security requirements are a complex set of system rules which, if violated can have serious repercussions. Verifying a given system's ability to meet its requirements is of increasing importance as dependency upon networked computer systems grows. Servicing multiple Network Aware Applications (NAAs) results in an operational environment that compounds verification complexity further. While an NAA may be free (or nearly free) from vulnerabilities as a stand-alone software component, it may present serious security risks when interacting other applications on a network. These vulnerabilities can be exploited with disastrous results.

Verification of network security system properties over concurrent processes (NAAs) is a problem well suited to model checking. However, the inherent complexity in these systems results in an intractable number of possible event combinations. This problem manifests itself as the "State Space Explosion" problem, which a known limitation of model checkers. This paper proposes an approach that mitigates this problem. The Flexible Modeling Framework (FMF) facilitates construction of a system model in a modular fashion with well-defined methods of interaction between processes. This allows a series of models to be efficiently created. Results from the FMF serve as input to a compositional analysis approach also proposed in this paper to verify properties over models, which would otherwise be beyond the capability of current state of the art model checkers.